

Enabling Secure Connectivity for Smart Meters



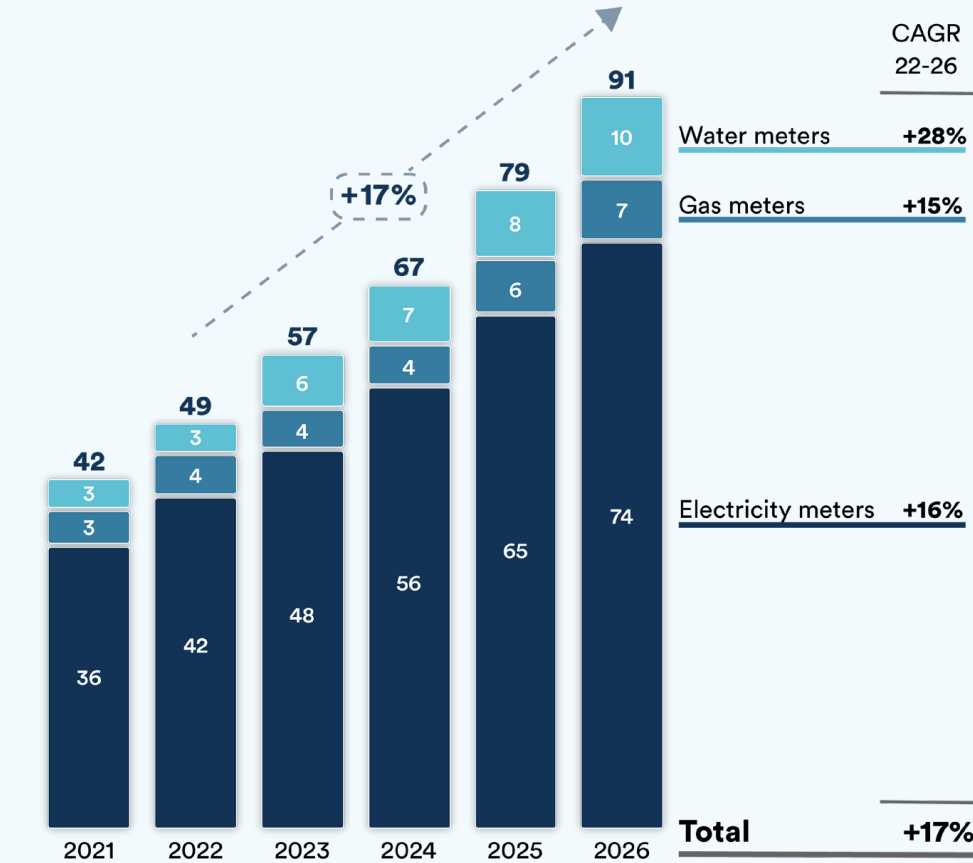
Smart metering set for rapid growth

Reducing the use of energy and water in homes and businesses is now a key factor in meeting the challenges of climate change and in reducing energy costs. Using smart meters, electricity, gas and water consumption can be closely monitored and managed to help achieve this. As a result, there is an increasing requirement to introduce smart meters globally. Growth in smart metering is high and is expected to continue at an overall fast pace of 17% per annum over the next few years. Within this overall figure smart water meters are destined for particularly strong growth of 28% per annum growth to 2026, followed by electricity at 16% per annum and gas at 15% per annum.

Monitoring and managing use of these resources requires more frequent data collection from smart meters. For utilities, this improves the frequency and reliability of invoicing. This frequency also serves to reduce the incidence of fraud, which in some cases can be substantial and up to 10% of revenues. Importantly, smart meter readings can also help to pinpoint the location of losses and leakages in the network. For water this may be up to 30% of the total resources available, and for gas up to 10%. Further, by analysing the patterns of usage, such data can also be used to prevent outages and shortages.

As shown in **Figure 1**, shipments of smart electricity meters represent the largest share at around 80% of the total throughout the period. Regulation in individual countries is a key driver, with utilities typically being required to install smart meters as part of government efforts to respond to climate change and increasing need to meet sustainability targets. Such regulations typically cover installation schedules (roll-out obligation), the need for security related to the data and the provision of in-home displays so their customers can monitor their usage in real time. The security solution typically needs to cover all aspects of the smart metering systems, including equipment used to communicate with those systems, associated software and ancillary devices, as well as related business processes.

Figure 1. Forecast of cellular smart meters annual shipments – worldwide excl. China (m units)



Source: Gartner

The top requirements for smart meter design

Utilities priorities for connected smart meters are reflected in **Figure 2**. This details the top 10 business user requirements regarding IoT devices and connectivity as researched by Arthur D. Little, and the most important of these for smart metering.

Utilities have particular high importance requirements for smart metering:











- **Regulatory Compliance**
- **Cost**
- **Security Features**
- **Quality of Coverage**
- **Device Lifetime**

Regarding Regulatory Compliance, utilities must comply with local security requirements, covering smart meter data, as well as meeting required installation schedules and the ability to change connectivity supplier.

Connectivity cost is usually around 10% per annum of the total initial cost of an electricity meter, so is a key factor in a large deployment of meters.

Each smart meter device must be secure. So must the data it generates. In addition, so must the connectivity to the smart meter system, since each meter can be the point of access for attack of the whole system. Utilities must also ensure that user data from smart meters is secure in relation to privacy concerns.

Figure 2. Utilities top requirements for smart metering

Utilities Requirements	Smart Metering	Key Facts / Comments
 Regulatory Compliance	High Importance	Needs to comply with local security requirements
 Cost	High Importance	Connectivity is usually c.10% p.a. of the total initial cost of an electricity meter
 Environmental Resilience	Medium Importance	High for water meters, lower for gas and electricity meters
 Ease of Installation	Low Importance	Usually installed by professionals, it takes ~5 days to install
 Bandwidth	Low Importance	Average low data usage (~100-150MB p.a.)
 Security Features	High Importance	Smart meters need to be secured as they can be the point of entrance for attackers into the entire utility system/grid
 Quality of Coverage	High Importance	High criticality to ensure continuity of service, especially for electricity meters
 Interoperability	Low Importance	As smart meters stay in place for up to 20 years, end Bs need to be able to change providers easily
 Device Lifetime	High Importance	Smart meters usually stay in place between 10 and 20 years. Water and gas meters usually battery power
 Contractual Model	Low Importance	Connectivity contracts with MNOs/MVNOs typically 5 years, so need to be able to swap operators during the device lifetime

Source: Arthur D. Little

Quality of connectivity coverage is critical for ensuring continuity of service. Smart meters must not become disconnected and there should be contingencies in place to ensure that does not happen.

The device lifetime of a smart meter is long, with typical life being 10 to 20 years. This means the device will likely need updates in the field, remote maintenance and other support that utilises the connectivity. Gas and water meters are also usually battery-powered, so the connectivity must have minimal impact on battery life.

Some of these requirements are highlighted in the following quotes from senior executives in the sector:

“Electricity meters are more at risk, as they connect to the entire system every 15 minutes on average, whilst water and gas meters usually only connect several times a year. Electricity utilities invest in security services, especially in the US where the market is fragmented.”

“As smart electricity meter data is critical to grid management, coverage reliability is an important factor. Smart meter manufacturers conduct meticulous network coverage success studies, in order to ensure highly reliable connectivity, even in unusual places such as basements.”

The challenge of designing these requirements into smart meters

Designing these requirements into smart meters involves taking into account the activities across the smart meter value chain that these devices serve. As illustrated in **Figure 3**, these activities start with the Device itself – how the smart meter is connected and secured involving choice of SIM*, chipset and cellular module. The choice of Connectivity needs to take into account provisioning requirements and initial setting up, as well as requirements for network operation. The Platform covers the connectivity management, which may or may not be carried out by the connectivity provider, and the device management for each smart meter. This stage also includes the data management, including storage of all the smart meter data. Finally, processing and analysing the data from all of the smart meters for maintenance and data analytics.

All of these activities must be capable of being carried out throughout the lifetime of the devices – and securely across the whole solution.



Note that the word 'SIM' in this paper is used in a generic sense. Depending on requirements, the specific type of SIM used could be a ruggedised SIM, eSIM or iSIM.

The key point here is that each of these activities is typically carried out by a different party along the value chain and each must be able to carry out their activities securely within the overall solution and throughout the device lifecycle. If not, the device will fail in the field. This puts great emphasis on the initial device design activity to cater for the needs of each of these stages.

Figure 3. Value chain for smart meters

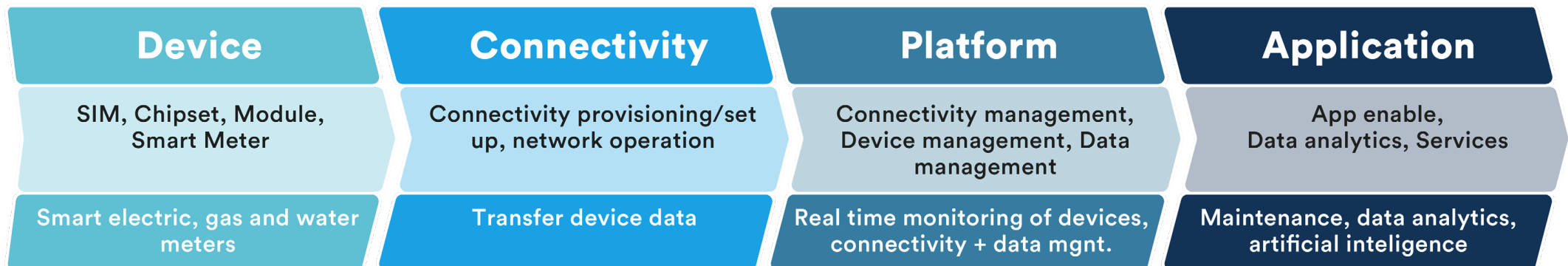
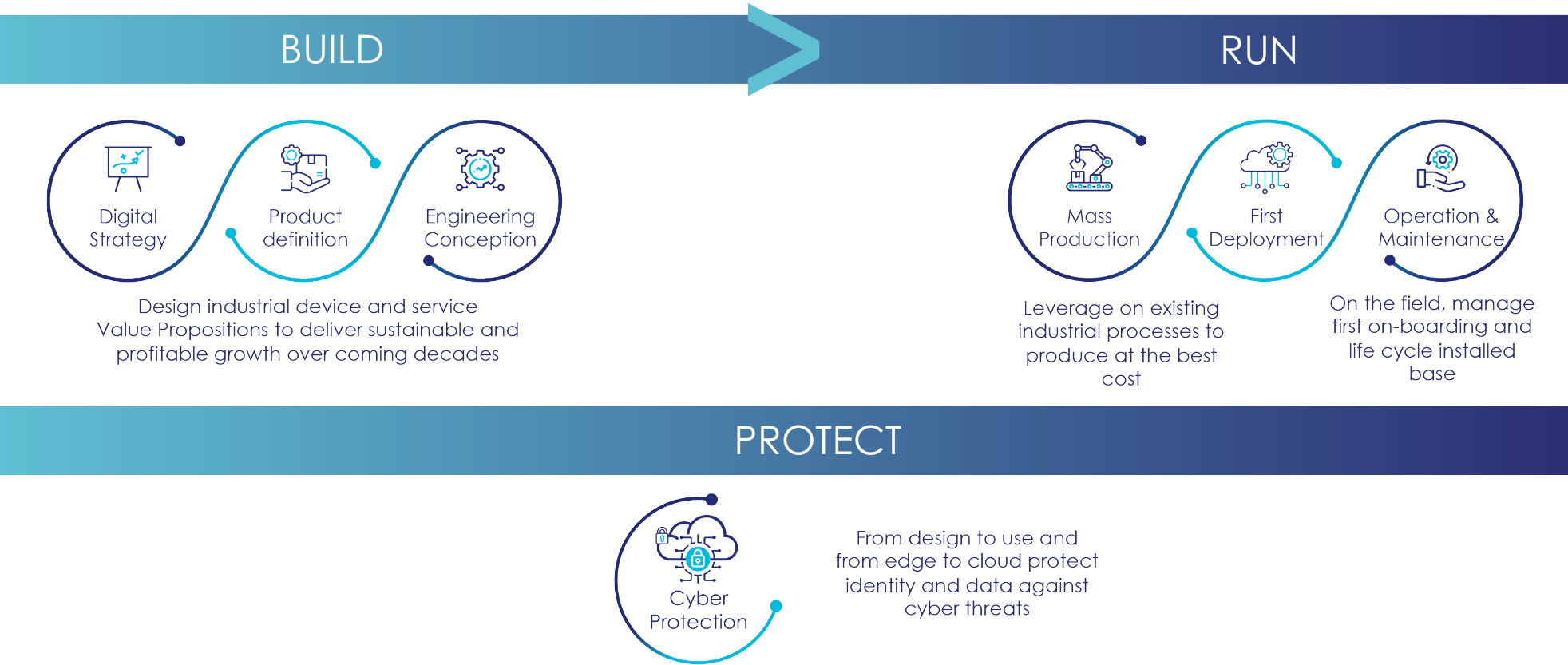


Figure 4. Thales Build – Run – Protect process for smart meter device designers



Thales has responded to these needs with a process for smart meter device designers called Build – Run – Protect, which is outlined in **Figure 4**.

Build is where the overall process starts and is where all the design decisions must be made, as it covers the initial digital

strategy, product concept and engineering design. According to Kaleido Intelligence, 84% of firms agree that the initial hardware design is their number 1 IoT challenge. It is the key stage for defining the connectivity choice, the level of security and other requirements to meet the business needs of the smart

meter solution. All of these then need to align with the Bill of Material (BoM) constraints.

Thales offers a range of industrial grade, standardised and future proof hardware SIMs to meet this challenge for smart meters, in order to match the operational constraints of power consumption, duration in the field and versatility while using cellular to securely connect the devices.

Run covers mass production, first deployment and then operation and maintenance for the device life in the field and subsequent decommissioning. According to Kaleido Intelligence, 51% of firms experience poor global connectivity with their IoT deployments. The need is for a solution allowing an efficient, open and resilient connectivity without impacting on manufacturing processes and costs. Thales SIMs and associated tools can simplify logistics with single Stock Keeping Units (SKUs) so that the SIM can be treated like any other discrete component for manufacturing purposes. In addition,

Thales tools can optimise roaming and coverage restrictions and save on costly human intervention of the SIM in the smart meter device in the field.

Protect covers the cybersecurity needs of smart meters and its data from the production line through to subsequent operation in the field. According to Kaleido Intelligence, 42% of firms consider that the security of devices through production and in the field is challenging. With large scale deployments of smart meters, the attack surface increases in line with the deployment size so the solution must be completely scalable. Thales offerings protect the device identity, shield data flows from edge to cloud and reinforce data sovereignty for critical assets.

How Thales meets smart meter top requirements

Figure 5 shows the Thales IoT portfolio that supports smart meter design requirements, comprising a wide range of SIMs, the Thales Connectivity Suite and the Thales Cyber Protection Suite.

With the high importance requirements that the Utilities have for Smart Metering noted earlier in mind, Thales products and services that support these are as follows:

As regards **Regulatory Compliance**, use of eSIM/iSIM provides a strong basis for meeting local security requirements covering smart meter data. In addition, these SIMs are designed to work seamlessly with IoT SAFE (SIM Applet For Secure End-to-End Communication) together with TKM (Trusted Key Manager) to extend this security from chip to cloud. eSIM/iSIM are also designed to optimise installation

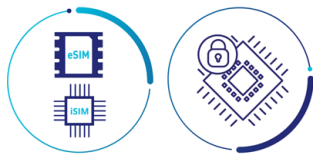
Figure 5. Thales IoT Offer Portfolio for Build – Run – Protect

BUILD

Range of industrial grade, standardized, futureproof hardware to securely connect devices.



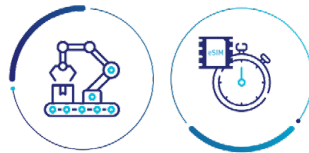
Ruggedized SIM
Mono & Multi Profile



SGP .32 xSIM
eSE

RUN

Connectivity Suite enabling a secure, global, resilient, cost-effective connectivity from production to operation.



In Factory Profile
Provisioning

Thales
Instant Connect

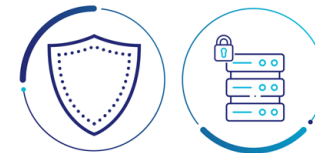


Thales
Adaptive
Connect

eSIM remote
provisioning

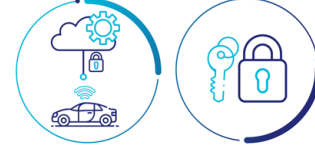
PROTECT

Cyber Protection Suite to protect IoT devices and data from factory to the field, from edge to cloud.



PQC

HSM



Thales IoT SAFE

Trusted Key
Manager

logistics and thereby assist the planning of consistent installation rates. The need to ensure smart meter connectivity is available at all times, together with the ability to change connectivity provider at scale, is provided by TAC (Thales Adaptive Connect).




































As regards **Cost**, iSIM together with TAC are suitable for low cost, low power NB-IoT deployments from both technical and cost perspectives. This is increasingly important, for example, for smart water meters that are battery-powered with a long field life, for which NB-IoT has been designed and is quickly ramping up.

As regards **Security Features**, IoT SAFE together with TKM facilitate deployment and life cycle management of credentials, which is key. As threats are evolving, so are security protection solutions. Also, eSIM and iSIM are hardware tamper proof elements.

As regards **Quality of Coverage**, eSIM/iSIM with TAC enables the ability to monitor coverage issues and to change the connectivity provider on a per device basis or at scale for fleets of devices as required.

As regards **Device Lifetime**, eSIM/iSIM have a very long lifespan that matches the requirements of utilities companies. Thales lifecycle management capabilities complement this to adapt fleets of devices to changing conditions over their lifetime of up to 20 years.

Figure 6. Summary of Thales offerings supporting Utility needs for connected smart meters

	 eSIM	 iSIM	 IoT SAFE	 TKM	 TAC
 Regulatory Compliance					
 Cost					
 Security Features					
 Quality of Coverage					
 Device Lifetime					

These Thales offerings in more detail:



1. Ruggedized SIM and eSIM/iSIM for the IoT

a. Key OEM and IoT SP challenges when designing, manufacturing and deploying cellular IoT devices:

- i. Robustness: the need to withstand extremes of temperature, humidity and vibration. IoT requires more ruggedized SIMs than those used in Consumer products.
- ii. Low power consumption: the need to accommodate battery-powered devices and cater for longer lifetimes in the field.
- iii. Optimized BoM and space: need for an optimized design and gaining space within the device.
- iv. Reliability, ability to operate over a long lifecycle without human intervention.
- v. Chip shortage: ability to manage this risk.

b. Key Thales product features that support these challenges:

- i. Ruggedized SIM for IoT: fully certified Ruggedized SIMs for industrial and low power IoT devices, targeted for MNOs and supporting single profile; available under various grades, formats, and OS options
- ii. eSIM/iSIM for IoT/MultiSIM: Fully GSMA certified multi-profile UICC with Remote SIM Provisioning (RSP) support.

- iii. Dedicated & performant IoT eSIM/iSIM OS and chipset
- iv. Different form factors from Removable (Plug 85; Plug 105) to Solderable (Quad) to ensure best fit with integration and operational needs.
- v. Services: end to end solution tested (hardware + connectivity enablement)

c. Why Thales is unique on the market: secure your IoT deployments with Thales:

- i. Long-standing IoT player, with over 600Mu embedded products shipped to mobile operators and OEMs, including automotive, smart utilities and more.
- ii. Limit chip shortage risk due to Multi sourcing capabilities (chipset in-house design; several silicon sources)
- iii. Benefit from unique expertise and support to integrate eSIM/iSIM in the devices



2. Thales Adaptive Connect

a. Key OEM and IoT SP challenges when manufacturing and deploying cellular IoT devices:

- i. Keeping TCO under control: throughout manufacturing/logistics processes.
- ii. Multiple SKUs when using local connectivity per country/region, leading to increased logistic costs and reduced scalability.
- iii. CSP lock-in prevents getting better rates and increases risk with changing roaming agreements and exposure to regulation constraints.
- iv. Permanent roaming forbidden in some countries limits business reach.
- v. Using M2M eSIM (SGP.02) is too complex and has strong limitations: high cost/long lead-time due to the mandatory interconnection of MNOs, SMS not supported by low power cellular technology (NB-IoT).
- vi. Future proof and scalable solution for usage and/or geographic evolution.

b. Benefits using Thales Adaptive Connect solution:

- i. Simple & fast access to the best local connectivity: no technical integration project, saving costs and months of delay.
- ii. Increased business agility and control: access to any CSP equipped with SM-DP+ (600 worldwide as of today), no technical dependency on current provider to swap to the new one.

iii. Cost-efficient and streamlined operating model with single SKU approach: one single eSIM for all deployments able to swap quickly to the selected connectivity provider.

iv. Enables low power use cases when needing 10+ years on a single battery charge: compatible with NB-IoT as SMS is not required.

v. Simple integration: Thales eSIM with IP Ae removes the need for developing specific software in the device.

vi. Implements the new GSMA SGP.32 standard for IoT

c. Why Thales is unique on the market:

TAC is the only commercial solution available that simplifies design, manufacturing and deployment of IoT devices to an unprecedented extent. The Thales eSIM-centric approach removes the effort of implementing specific software in the device, and the cost of investing in secure manufacturing while providing the full flexibility of eSIM for connectivity management.



3. Thales Instant Connect

a. Key Industrial and Consumer IoT OEM and module vendor challenges when manufacturing and deploying cellular IoT devices with eSIM and targeting multiple Telco Operators:

- i. IoT devices are constrained, with no screen, no keyboard, it is not possible from the device itself to setup a Wifi connection or download an eSIM profile, among other actions. Devices need to come from the factory ready to connect, without human intervention.
- ii. Ready to connect means, the device needs to come out of the factory with the Telecom Operator profile inside. This results in multiple eSIM SKUs, one per Telecom Operator
- iii. Multiple eSIM SKUs adds complexity and costs to the eSIM supply chain and stock management and device manufacturing and logistics.
- iv. Slow device commercialization, as device manufacturing depends on knowing in advance the Telecom Operator for each device.

b. Benefits using Thales Instant Connect:

- i. Simplification at every step, from the eSIM supply chain and stock management, to the device manufacturing and deployment, by having one eSIM SKU that can be integrated into all devices and containing Thales' initial worldwide cellular connectivity service.

- ii. Flexibility and acceleration of device commercialization, by making devices more generic and suitable for multiple customers and Telecom operators.
- iii. Best user experience, not dependent on Bluetooth, for Consumer IoT device activation
- iv. Save profile preloading costs: USD cost per eSIM typically charged by the eSIM vendors when supplying eSIM with preloaded profiles.
- v. Avoid integrations and complexities linked to the activation/termination of the initial connectivity subscriptions.
- vi. Simplifying your supply chain, with Thales as the one-stop-shop, providing both the eSIM and the initial connectivity.

c. Why Thales Instant Connect is unique:

Thales Instant Connect is a game changer for OEMs wanting to equip devices with eSIM. It helps them to stay focused in their core device-making activities rather than in the eSIM connectivity.

The OEM simply embeds the eSIM during manufacture and does not need to take care of activating and terminating the subscriptions later on. This removes the implicit complexities of tracking which subscription is inside each device and their management. These two novelties are a game changer.



4. Thales IoT SAFE

a. IoT SPs consider security as #1 challenge in IoT and OEMs struggle to respond efficiently:

- i. Rapidly evolving security threats: increasing attack surface of connected devices leading compromised IoT devices being used to launch DDoS attacks, identity breaches, and data theft.
- ii. Costly/Difficult to implement and maintain: traditional solutions are either not effective enough (software based) or costly in terms of resources, design, manufacturing (secure element based)
- iii. Regulations are on the rise: initiatives in EU and US putting more emphasis on digital security in connected objects and liabilities of solution providers.
- iv. Lack of skilled workforce: scarce availability and defocus from core business.

b. OEM-IoT SP benefits using Thales solution:

- i. High security level: credentials stored in the eSIM, the industry acknowledged (and standardized) tamper resistant element (TRE).
- ii. Cost efficient and hassle-free integration: no impact on BOM nor manufacturing infrastructure and processes as it reuses certified secure platform (eSIM or iSIM) already present in the cellular device
- iii. Multipurpose solution to protect device and identity breaches and data leakage all along device life cycle.

iv. Evolutive: to cope with cyber threats evolution and scalable with no impact on cost whatever the number of devices deployed.

v. Under OEM/IoT SP's control: security services independent from connectivity provider, secure cloud communication is always available.

c. Superiority: For large scale IoT deployment no more compromise over security and cost.

IoT SAFE and its touchless provisioning service by Thales is the only solution allowing IoT OEMs to manufacture highly secured devices without modifying their production infrastructure and processes and still get top-notch cyber protection on the field.

Thanks to Thales unique remote management expertise activate, customize and manage over time your cyber security credentials OTA once your device is on the field.



5. Trusted Key Manager

a. Challenges for CISO of companies using connected devices (whatever connectivity technology):

- i. IoT Trust: Fleet of connected devices in the field expand the surface of attack. How to ensure we can trust device identity and security?
- ii. Prevent Cyber Attacks: protect against increasingly malicious activities. Theft of data. Loss of business. Criminal or geo-political related hacking activities
- iii. To comply with regulations or obtain certifications, need to prove a correct level of long-term security on devices.
- iv. Multiplicity of device vendors. Complexity is introduced with each device vendor's proprietary device security solution.
- v. Long term cryptographic evolution. Ensure state of the art security for devices which will be deployed for the next 20 years or more.

b. Benefits of using Thales Trusted Key Manager:

- i. Pre-built platform managing devices identities and secrets through a root of trust (PKI) and a comprehensive device identity database.
- ii. Advanced state of the art security backed by Thales Luna HSM with ensured evolution of cryptography over time.
- iii. Centrally generate, provision and manage device identities and secrets for the whole device life cycle.
- iv. Control roles per use cases and multi-vendor schemes.

c. Why TKM by Thales is unique:

- i. Most comprehensive, device vendor agnostic, IoT Cyber Security platform backed by the best-in-class HSM cryptography also by Thales.
- ii. Pre-implemented flexible platform going from a KMS to a complete IoT device security system with Certification Authority and device security database. Avoids years of specific developments.

Summary

Responding to the growing challenges of resource conservation and climate change, utilities are now introducing smart metering for electricity, gas and water at a fast rate. Their most important requirements for connected smart meters relate to: regulatory compliance, cost, security features, quality of connectivity coverage and device lifetime in the field.

When building smart meter systems, these requirements must be catered for during the initial design stage for the overall system to work effectively and securely in

the field. Thales has responded to these needs with a process for smart meter device designers called **Build, Run, Protect**.

Of these, the Build stage is where the overall process starts and is where all the design decisions must be made. Thales has created a range of market leading products and services to implement these design decisions for each of the most important requirements of the utilities across the whole smart meter solution.



Case Study - Utilities Smart Water

Context

With the increasing need to conserve water and with the effects of climate change, there is an increasing need for smart water meter deployments for water utilities. These have a long life of more than 15 years in the field with no external power and, for a particular utility, may be deployed in multiple countries.

The cellular technology used for the connectivity is low data rate and low power NB-IoT. This must operate effectively for a minimum period of 10 years on a single battery charge.

The Problem

There is a gap between the normal contract period for cellular connectivity and the field life of a smart meter. As a result, there may be a need to change network profiles in the field. On the other hand, downloading the first profile remotely uses battery power that many utilities would like to avoid.

Solution with Thales Adaptive Connect (TAC)

To avoid downloading the first profile remotely, TAC allows for provisioning it in the device at the factory – termed In Factory Profile Provisioning (IFPP). This enables the manufacture of a single SKU which can then be personalised at the very last stage with the initial network operator profile that is the right one for the site where the meter will be deployed. When installed, the smart meters are activated and use the network profile already installed. If a subsequent change of profile is required as a result of a new connectivity contract negotiation, this can be managed remotely through TAC.

